J. Symbolic Computation (1997) **23**, 453–458

A Use of Computers to Teach Group Theory and Introduce Students to Research

NIGEL BOSTON†

Department of Mathematics, University of Illinois, Urbana, IL 61801, U.S.A.

(Received 31 July 1995)

This paper describes a graduate course in which students explored unsolved problems in group theory by computer. This introduced them both to the subject and to the use of computational software in doing research. One outcome was a joint publication by the class.

1. Introduction

This is a report on a one-semester course given at the University of Illinois at Urbana-Champaign in the fall of 1991. The course was entitled "Computational Group Theory" and was intended to introduce students both to group theory and to the use of computational software in doing research. In this case the software system was CAYLEY (which has now been developed into the broader computer algebra system MAGMA), but it is clear that this approach would work with other systems. In particular, using PARI-GP, I gave a similar course on "Elliptic Curves by Computer" in the fall of 1994, which will be described towards the end of this paper.

The approach consisted of exploring problems to which the students (and often I) did not know the answer. There were approximately 11 students, ranging from ones with little more than Sylow theory to authors of well-known group theory textbooks. We worked in a room with enough Sun workstations, with me wandering around, answering and asking questions. Occasionally I would write some computational or theoretical tool up on the board, as needed, and sometimes one of the students would present something they had discovered. It was very informal with a great sense of team spirit, of us against the problem. The problems came from a variety of sources and I shall describe the history of our progress with the second one we attempted, kindly suggested by Hendrik Lenstra. It had arisen a little earlier in his work on the number field sieve. Indeed, the joint paper Boston *et al.* (1993) we produced as a class from our discoveries is referenced in Buhler *et al.* (1994).

Much of what follows has been culled from notes that I handed out each week in order to keep track of our discoveries, questions and conjectures. I used these to mention

† E-mail: boston@math.uiuc.edu

0747–7171/97/050453 + 06 $25.00/0 sy960100

Table 1. f for small degree.

Degree 2	$f(S_2) = 0.500$
Degree 3	$f(A_3) = 0.667$
	$f(S_3) = 0.333$
Degree 4	$f(C_4) = 0.750$
	$f(C_2 x C_2) = 0.750$
	$f(D_8) = 0.625$
	$f(A_4) = 0.250$
	$f(S_4) = 0.375$
Degree 5	$f(C_5) = 0.800$
	$f(D_{10}) = 0.400$
	$f(\mathrm{Hol}(C_5)) = 0.200$
	$f(A_5) = 0.400$
	$f(S_5) = 0.366$

relevant pieces of theory and techniques from CAYLEY and to keep the students focused on what was known (and not known) so far.

2. The Course

The problem that Lenstra suggested was the following:

Problem. Let G be a transitive permutation group on n letters (i.e. given any letters x, y, there is an element of G that sends x to y). Let A be the subset of elements of G that move every letter. Find a good lower bound (in terms of n) for $|A|/|G|$.

We shall denote this ratio by $f(G)$ (although it should be noted that this notation is a little abusive since the ratio also depends on the embedding of G in S_n—for instance S_3 can be considered as acting on six letters, namely its own elements).

The first thing we did was to write procedures that would take a small value of n, find all subgroups of S_n, pick out the transitive ones, and then calculate the corresponding values of $f(G)$. Above is a table of the results obtained (to three decimal places) for small n.

Before continuing, the readers may like to put themselves in the position of the students in the course and see what observations they can make regarding the values of f and in particular Lenstra's question.

We actually found it feasible to go as far as $n = 7$ by this admittedly inefficient method. From this we realized that $f(G) > 0$ always, since A is the complement of a union of conjugate subgroups and an old well-known counting argument tells us A is non-empty (this is sometimes called the Cauchy–Frobenius lemma). Looking at our tables suggested that $1/n$ would answer Lenstra's question. In addition some people noted that $f(S_n)$ and $f(A_n)$ seemed to hover around 0.367 for large n.

This produced some new questions, namely:

(1) For which n and which groups G does $f(G)$ actually equal $1/n$?
(2) What are the accumulation points of $\{f(G) : G \text{ is a transitive permutation group}\}$?

It was not long before we found a quicker way to calculate f by simply noting that A is

a union of conjugacy classes, meaning that we just had to run through representatives of these rather than every element of the group. For $f(S_{10})$ the old way took about 2.5 days, whereas the new way took 4 seconds. This made a big impression on students who were becoming perhaps too reliant on the machine. Here is the CAYLEY procedure we used:

```
procedure quk(g);
n=0;
k=classes(g;al:random);
for i=1 to length(k) do
if fix(k[i]) eq null then
n=n+fetch(k,i;length);
end;
end;
print n,n*10000/order(g);
end;
```

The CAYLEY language is very self-explanatory. We are simply checking whether a representative $k[i]$ of the ith conjugacy class has a null fixed-point set. Since CAYLEY only does integer arithmetic, we must multiply by 10 000 at the end to get $f(G)$ (times 10 000).

Someone realized that 0.367 is approximately $1/e$ and that the fact that $f(S_n)$ tends to $1/e$ as $n \to \infty$, is the old well-known derangement problem, proven by means of the inclusion–exclusion principle. A minor adaptation of this showed that $f(A_n) \to 1/e$ as well.

As for our new question (1), an analysis of all the groups G of degree n with $f(G) = 1/n$ revealed certain common features. In particular they seemed to exist only for n a prime power, say $n = p^r$, and in this case there was apparently a unique group $G(n)$, where $G(n)$ was an extension of a normal Sylow subgroup K isomorphic to $C_p \times \cdots \times C_p$ by a cyclic group of order $n-1$ (here commands such as

```
k=sylow(g,p); print abelian(k); print exponent(k); print exponent(g/k);
```

led to these conclusions). By Schur–Zassenhaus, this extension is split, meaning that $G(n)$ has a subgroup H mapping isomorphically onto $G(n)/K$. We found that the corresponding action is fixed-point-free, meaning that no non-trivial element of H conjugates a non-trivial element of K to itself. In other words we had identified $G(n)$ as the Frobenius group

$$F_n := \{x \mapsto ax + b : a, b \in GF(n), a \neq 0\}.$$

(We did not realize it at the time but for certain prime powers n there exist Frobenius groups G not isomorphic to F_n with $f(G) = 1/n$.) It was easy to see that there are transitive subgroups G of F_n with $f(G) = d/n$, for any divisor d of $n-1$. It follows that, as regards our new question (2), the accumulation points obtained to date were $0, 1/n$ (any positive integer n), and $1/e$.

By now we had discovered the libraries of transitive groups (of degree up to 12) and primitive groups (of degree up to 50) that came with CAYLEY (called up e.g. by `library t6n2;` or `library p50n3;`). One of the faculty members attending the course was having problems sleeping at night and kindly spent these hours working his way through these libraries so that we soon had the useful resource of almost complete tables of values of f

for the groups listed above. The tables missed out some very large groups but by having the computer randomly select many thousands of elements (using `x=ranelt(g);`) we could get excellent estimates for f for these groups too. These tables led us to notice, for instance, that there were a few values of f clustering around 0.6065.

In the meantime we found a quick proof that for transitive groups G of prime degree p, $f(G) \geq 1/p$. This came from seeing that p-cycles are always in A and that we can easily count the p-cycles in G.

Going back to the accumulation points, we calculated f for various natural sequences of groups (inspired by S_n, A_n) and noticed that, for instance, $f(GL(n,2)) \to 0.288\,788\ldots$ as $n \to \infty$, $GL(n,2)$ being the group of invertible n by n matrices over the field of two elements (`general linear(n,field(2));` in CAYLEY). I contacted John McKay, having been told he was good at identifying numbers. He pointed out in a one-line e-mail message that

$$\prod_{k=1}^{\infty}(1-2^{-k}) = 0.288\,788\,095\ldots.$$

I later discovered that Washington (1986) had in effect proven that $f(GL(n,2))$ tends to this. Also Bernoulli had considered this product back in 1713. As for 0.6065, you may have already identified this as approximately $e^{-1/2}$. This led me to conjecture that the set of accumulation points is of the form

$$\{h(1/n) : h \in \Sigma, n \in \mathbb{Z}^+\},$$

where $\Sigma = \{x, e^{-x}, p(x) = \prod_{k=1}^{\infty}(1-x^k), \ldots\}$ is some set of functions.

We next analysed groups G with $f(G)$ very close to $e^{-1/2}$. We found that they all belonged to a sequence of groups $G(m)$ of even degree $2m$, with a normal subgroup $K \cong C_2 \times \cdots \times C_2$ (m times) and quotient $G(m)/K \cong S_m$. This extension turned out to be split with S_m acting in its natural way on the m natural generators of K. This enabled me to introduce the theory of blocks of imprimitivity (meaning a set of letters that each group element maps either to itself or to a non-intersecting set) and the theory of the wreath product, something not planned at the outset. Indeed what I described above is the fact that $G(m) \cong C_2 \wr S_m$ (in CAYLEY, `wreath(cyclic(2),symmetric(m));`). Next, by modifying the inclusion–exclusion principle, some students (ones with little more than Sylow theory in the beginning) found that they could prove that $f(C_n \wr S_m) \to e^{-1/n}$ as $m \to \infty$. They described this as instilling a great feeling. In fact, at this point, the students were so engrossed in the work that there would be several of them in the computer room playing around with it at apparently all times of the day.

In addition to the progress we made, we were regularly coming up with conjectures, several of which were listed at the end of Boston *et al.* (1993) and some of which are still open today. For example, if G is a simple group, does $f(G) \geq 2/7$ always hold? There are two examples of simple groups G with $f(G) = 2/7$.

At last, a student managed to prove that $f(G) \geq 1/n$ with equality if and only if n is a prime power and G is a Frobenius group of order $n(n-1)$, answering Lenstra's question and our question (1). This was proven previously by Cameron and Cohen (1992) by a different method.

After exploring $f(G \wr S_m)$ for various groups G and applying our modified inclusion–exclusion principle, we proved that $f(H \wr K) = p_K(f(H))$, where $p_G(t) = (\sum_{i=0}^{n} m_i t^i)/|G|$ with $m_i =$ the number of elements of G that fix exactly i letters. The invariant p_G turned out to have many useful properties. For example, if H and K act on sets X and Y

respectively, then letting $H \wr K$ and $H \times K$ act on $X \times Y$ and $X \coprod Y$ respectively, then $p_{H \wr K}(t) = p_K(p_H(t))$ and $p_{H \times K}(t) = p_H(t)p_K(t)$. In other words, the p_G turns natural compositions of permutation groups into natural compositions of polynomials. Under this, taking one-point stabilizers corresponded to differentiating. We did not realize at the time that $p_G(t)$ is the specialization $z_1 = t$ and $z_i = 1$ for $i > 1$ of the cycle indicator polynomial (of Polya and Redfield) $C(G, \underline{n}) = (\sum_{g \in G} \prod_{i=1}^{n} z_i^{a_i(g)})/|G|$, where $a_i(g)$ denotes the number of i-cycles of the element $g \in G \leq S_n$ [see Kerber (1991)].

This led, not long thereafter, to a proof that $\{f(G) : G$ is a transitive permutation group$\}$ is dense in $[0, 1]$, answering our question (2). Picking $\epsilon > 0$, there exists a prime power $n > 1/\epsilon$ and hence a group G_1 with $f(G_1) = 1/n < \epsilon$. Defining $G_k = G_{k-1} \wr G_1$, the properties of p_G together with the Mean Value Theorem enabled us to show that $\{f(G_k)\}$ is ϵ-dense in $[0, 1]$.

In fact, further investigation of the literature revealed that there was also a method of producing new primitive groups (i.e. groups with no non-trivial blocks of imprimitivity) from old ones. The idea is that if H and K are primitive, acting on X and Y respectively, and $H \neq C_p$ for some prime p, then $H \wr K$ considered as acting on X^Y (the so-called product action) is also primitive. We therefore sought out a polynomial invariant q_G such that $f(H \wr K)$ (with the product action) $= q_K(f(H))$ and likewise deduced this $\{f(G) : G$ is a primitive permutation group$\}$ is dense in $[0, 1]$. One can in fact restrict this to even more specialized families of groups, but in each case the method is essentially the same.

Actually, some of the above was discovered after we had decided to move on to some other problems, so as to explore fully the group theory and the range of CAYLEY computational tools. For grading purposes the students were told to investigate one or more of the loose ends from the Lenstra question and to write up and hand in a report on their work. We then met, after the course had finished, and put it all together in a paper. The students thus got practice writing and submitting a research paper. It was accepted and became Boston *et al.* (1993).

3. Further Developments

The feedback from the course was very encouraging. When asked in a student evaluation of the course to say what aspects of the course were most beneficial to them, some of the students with weaker backgrounds said "Seeing that it is not beyond my ability to be on the frontier of a subject" and "The encouragement to <u>do</u> research, rather than just read other people's results".

The outgrowths of this course were several. While it apparently did not, except in one case, draw students into group theory for their PhD work, it did get them interested in using CAYLEY. In a handful of papers, CAYLEY was employed if only in a subsidiary role of checking results. I used it in my own work in algebraic number theory. If we need to know, as happened recently in a seminar, that $SL(2, 3)$ has no subgroup of order 12, then a student might have CAYLEY do it *and stop there*. The temptation to replace understanding with machine computation is great.

As I mentioned in my introduction, in the fall of 1994 I attempted a course on elliptic curves at the University of Illinois, following the same approach as detailed above. This attracted about 20 students and was conducted in the same, informal manner. The students learned a lot about elliptic curves and PARI-GP, but, although we made progress on some of the problems, none of this made it into print as a joint work. (It has, however, produced papers by individuals and also references to be made in other people's work.) As

some students remarked to me later, a lot of people signed up for the course anticipating something similar to what happened in the earlier course. This made for uncomfortable pressure. The reason why we did not attain the full success of the first course is that firstly I did not have a problem as promising as Lenstra's and secondly elliptic curves do not provide an area as forthcoming in problems as group theory. It seemed that many problems on elliptic curves led to standard unsolved conjectures. Since giving the course I have come across questions that may have worked better. As advice for anyone attempting this approach to teaching, if you wish to go all the way (i.e. to obtain a publication), make sure that you have a supply of good problems ready in advance. Even if publications do not materialize, this method is highly recommended for teaching (and learning).

References

Boston, N., Dabrowski, W., Foguel, T., Gies, P.J., Jackson, D.A., Leavitt, J., Ose, D.T. (1993). The proportion of fixed-point-free elements of a transitive permutation group. *Comm. in Alg.* **21**(9), 3259–3275.

Buhler, J.P., Lenstra, H.W., Pomerance, C. (1994). Factoring integers with the number field sieve *Lecture Notes in Math.* **1554**.

Cameron, P.J., Cohen, A.M. (1992). On the number of fixed point free elements in a permutation group. *Annals of Discrete Math.* **106/107**,135–138.

Kerber, A. (1991). Algebraic combinatorics via finite group actions, BI Wissenschaftsverlag, Mannheim/Wien/Zürich.

Washington, L.C. (1986). Some remarks on Cohen–Lenstra heuristics. *Math. Comp.* **47**, 741–747.